

What is claimed is:

1. A computer which comprises a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, wherein

said system section judges that said application software section is legitimate application software for the protection of copyright, and

if said application software is a legitimate one, said system section passes a key for said encrypted data to said application software section.

2. A computer as set ^{forth} ~~fourth~~ in claim 1, wherein said judgement in said system section is made by performing authentication between said system section and said application software section.

3. A computer as set ^{forth} ~~fourth~~ in claim 1, wherein said judgement in said system section is made by using a CRL (Certification Revocation List) listing illegitimate or legitimate application software.

4. A computer as set ^{forth} ~~fourth~~ in any one of claims 1 to 3, wherein said system section obtains said encrypted key as the result of authentication with an external device, decrypts said encrypted data, and re-encrypts said decrypted data by using said key or another key.

5. A computer as set ^{forth} ~~fourth~~ in any one of claims 1 to

3
4, wherein said system section includes a tamper verification function, and a tamper code is embedded into said application software in said application software section, and wherein said system section reads said tamper code from said application software section and, using said tamper verification function, verifies whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, said system section reports the result of said verification.

6. A computer which comprises a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, wherein

said system section includes a plurality of tamper verification functions, and a tamper code associated with a designated type of tamper verification function and type information indicating said type are embedded into said application software in said application software section, and wherein said system section reads said tamper code and its associated type information from said application software section and, using the tamper verification function corresponding to said type, verifies whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, said system section reports the result of said verification.

7. A computer which comprises a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, wherein

said system section sends said data to said application section by embedding into said data information concerning application software residing in said application software section.

8. A computer as set ^{forth} ~~fourth~~ in claim 7, wherein the information concerning said application software is information indicating the name of said application software, or the version number of said application software, or a tamper code, or the type of a tamper resistance verification function, or information concerning user.

9. A medium holding thereon a program and/or data for enabling a computer to implement all or part of the functions of all or part of the means of the invention described in any one of the claims 1 to ^{2, 3, 6, 7, or 8} 8, wherein said medium is computer processable.

10. A collection of information wherein said collection of information is a program and/or data for enabling a computer to implement all or part of the functions of all or part of the means of the invention described in any one of the claims 1 to ^{2, 3, 6, 7, or 8} 8.

add
B1